



CVE-2022-38751

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-38751
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-05 10:15:00 UTC
Updated	2024-03-15 11:15:00 UTC
Description	Using snakeYAML to parse untrusted YAML files may be vulnerable to Denial of Service attacks (DOS). If the parser is run

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Snakeyaml Project	Snakeyaml	All	All	All	All

References

Reference	Source	Link	Tags
snakeyaml: Multiple Vulnerabilities (GLSA 202305-28) — Gentoo security	GENTOO	security.gentoo.org	
snakeyaml / snakeyaml / issues / #530 - Stackoverflow [OSS-Fuzz - 47039] — Bitbucket	MISC	bitbucket.org	
security.netapp.com/advisory/ntap-20240315-0010		security.netapp.com	
47039 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	
[SECURITY] [DLA 3132-1] snakeyaml security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181092](#) Debian Security Update for snakeyaml (DLA 3132-1)

184250 Debian Security Update for snakeyaml (CVE-2022-38751)
199232 Ubuntu Security Notification for SnakeYAML Vulnerabilities (USN-5944-1)
20396 IBM DB2 Multiple Vulnerabilities (7095807)
241405 Red Hat Update for Satellite 6.13 (RHSA-2023:2097)
710729 Gentoo Linux snakeyaml Multiple Vulnerabilities (GLSA 202305-28)
753357 SUSE Enterprise Linux Security Update for snakeyaml (SUSE-SU-2022:3397-1)
903881 Common Base Linux Mariner (CBL-Mariner) Security Update for snakeyaml (10867)
960924 Rocky Linux Security Update for Satellite (RLSA-2023:2097)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)